1311.45 Requirements for registrants that allow powers of attorney to obtain CSOS digital certificates under their DEA registration.
1311.50 Requirements for recipients of digitally signed orders.
1311.55 Requirements for systems used to process digitally signed orders.
1311.60 Recordkeeping.

AUTHORITY: 21 U.S.C. 821, 828, 829, 871(b), 958(e), 965, unless otherwise noted.

SOURCE: 70 FR 16915, Apr. 1, 2005, unless otherwise noted.

EFFECTIVE DATE NOTE: At 70 FR 16915, Apr. 1, 2005, part 1311 was added, effective May 31, 2005.

Subpart A—General

§ 1311.01 Scope.

This part sets forth the rules governing the use of digital signatures and the protection of private keys by registrants.

§ 1311.02 Definitions.

For the purposes of this chapter:

Biometric authentication means authentication based on measurement of the individual's physical features or repeatable actions where those features or actions are both unique to the individual and measurable.

Cache means to download and store information on a local server or hard drive.

Certificate Policy means a named set of rules that sets forth the applicability of the specific digital certificate to a particular community or class of application with common security requirements.

Certificate Revocation List (CRL) means a list of revoked, but unexpired certificates issued by a Certification Authority.

Certification Authority (CA) means an organization that is responsible for verifying the identity of applicants, authorizing and issuing a digital certificate, maintaining a directory of public keys, and maintaining a Certificate Revocation List.

CSOS means controlled substance ordering system.

Digital certificate means a data record that, at a minimum:

(1) Identifies the certification authority issuing it;

(2) Names or otherwise identifies the certificate holder;

(3) Contains a public key that corresponds to a private key under the sole control of the certificate holder;

(4) Identifies the operational period; and

(5) Contains a serial number and is digitally signed by the Certification Authority issuing it.

Digital signature means a record created when a file is algorithmically transformed into a fixed length digest that is then encrypted using an asymmetric cryptographic private key associated with a digital certificate. The combination of the encryption and algorithm transformation ensure that the signer's identity and the integrity of the file can be confirmed.

Electronic signature means a method of signing an electronic message that identifies a particular person as the source of the message and indicates the person's approval of the information contained in the message.

FIPS means Federal Information Processing Standards. These Federal standards, as incorporated by reference in §1311.08, prescribe specific performance requirements, practices, formats, communications protocols, etc., for hardware, software, data, etc.

FIPS 140–2, as incorporated by reference in §1311.08, means a Federal standard for security requirements for cryptographic modules.

FIPS 180–2, as incorporated by reference in §1311.08, means a Federal secure hash standard.

FIPS 186–2, as incorporated by reference in §1311.08, means a Federal standard for applications used to generate and rely upon digital signatures.

Key pair means two mathematically related keys having the properties that:

(1) One key can be used to encrypt a message that can only be decrypted using the other key; and

(2) Even knowing one key, it is computationally infeasible to discover the other key.

NIST means the National Institute of Standards and Technology.

Private key means the key of a key pair that is used to create a digital signature.

Public key means the key of a key pair that is used to verify a digital signature. The public key is made available to anyone who will receive digitally signed messages from the holder of the key pair.

Public Key Infrastructure (PKI) means a structure under which a Certification Authority verifies the identity of applicants, issues, renews, and revokes digital certificates, maintains a registry of public keys, and maintains an up-to-date Certificate Revocation List.

§ 1311.05 Standards for technologies for electronic transmission of orders.

(a) A registrant or a person with power of attorney to sign orders for Schedule I and II controlled substances may use any technology to sign and electronically transmit orders if the technology provides all of the following:

(1) *Authentication:* The system must enable a recipient to positively verify the signer without direct communication with the signer and subsequently demonstrate to a third party, if needed, that the sender's identity was properly verified.

(2) *Nonrepudiation:* The system must ensure that strong and substantial evidence is available to the recipient of the sender's identity, sufficient to prevent the sender from successfully denying having sent the data. This criterion includes the ability of a third party to verify the origin of the document.

(3) *Message integrity:* The system must ensure that the recipient, or a third party, can determine whether the contents of the document have been altered during transmission or after receipt.

(b) DEA has identified the following means of electronically signing and transmitting order forms as meeting all of the standards set forth in paragraph (a) of this section.

(1) Digital signatures using Public Key Infrastructure (PKI) technology.

(2) [Reserved]

§ 1311.08 Incorporation by reference.

(a) The following standards are incorporated by reference:

(1) FIPS 140–2, Security Requirements for Cryptographic Modules, May 25, 2001, as amended by Change Notices 2 through 4, December 3, 2002.

(i) Annex A: Approved Security Functions for FIPS PUB 140–2, Security Requirements for Cryptographic Modules, September 23, 2004.

(ii) Annex B: Approved Protection Profiles for FIPS PUB 140–2, Security Requirements for Cryptographic Modules, November 4, 2004.

(iii) Annex C: Approved Random Number Generators for FIPS PUB 140–2, Security Requirements for Cryptographic Modules, January 31, 2005.

(iv) Annex D: Approved Key Establishment Techniques for FIPS PUB 140–2, Security Requirements for Cryptographic Modules, February 23, 2004.

(2) FIPS 180–2, Secure Hash Standard, August 1, 2002, as amended by change notice 1, February 25, 2004.

(3) FIPS 186–2, Digital Signature Standard, January 27, 2000, as amended by Change Notice 1, October 5, 2001.

(b) These standards are available from the National Institute of Standards and Technology, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899–8930 and are available at *http://csrc.nist.gov/*.

(c) These incorporations by reference were approved by the Director of the Federal Register in accordance with 5 U.S.C. 552(a) and 1 CFR part 51. Copies may be inspected at the Drug Enforcement Administration, 600 Army Navy Drive, Arlington, VA 22202 or at the National Archives and Records Administration (NARA). For information on the availability of this material at NARA, call (202) 741–6030, or go to: *http://www.archives.gov/federal__register/code__of__federal__regulations/ibr__locations.html*.

Subpart B—Obtaining and Using Digital Certificates for Electronic Orders

§ 1311.10 Eligibility to obtain a CSOS digital certificate.

The following persons are eligible to obtain a CSOS digital certificate from the DEA Certification Authority to sign electronic orders for controlled substances.